UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/654,417	09/04/2003	Philip Kwan	FOUND-0058 (434103-049)	7628

49680 7590 09/04/2009

FOUNDRY-NIXON PEABODY LLP
200 Page Mill Road
Palo Alto, CA 94306

EXAMINER	
ABEDIN, SHANTO	

ART UNIT	PAPER NUMBER
2436	

MAIL DATE	DELIVERY MODE
09/04/2009	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/654,417	KWAN ET AL.	
	Examiner	Art Unit	
	SHANTO M. ABEDIN	2436	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *03* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *29 June 2009*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-46* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-46* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *04 September 2003* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date *07/08/2009*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on 06/29/2009 has been entered.

2. Claims 1-46 have been presented for examination.

3. Claims 1-46 have been rejected.

4. The examiner notes, upon further examination, new grounds of obviousness type Double Patenting rejections are found, and presented in this office action.

Response to Arguments

5. The applicant's arguments regarding 35 USC 101 type rejections fully considered, and found persuasive. The previous 35 USC 101 type rejections of claims 1-12, 35, 38-39 and 44 are withdrawn.

6. The applicant's arguments regarding the previous 35 USC 103(a) type rejections are fully considered, however, moot in view of new grounds of rejections presented in this office action.

Double Patenting

The nonstatutory double patenting rejection is based on a judicially created doctrine grounded in public policy (a policy reflected in the statute) so as to prevent the unjustified or improper timewise extension of the "right to exclude" granted by a patent and to prevent possible harassment by multiple assignees. See *In re Goodman*, 11 F.3d 1046, 29 USPQ2d 2010 (Fed. Cir. 1993); *In re Longi*, 759 F.2d 887, 225 USPQ 645 (Fed. Cir. 1985); *In re Van Ornum*, 686 F.2d 937, 214 USPQ 761 (CCPA 1982); *In re Vogel*, 422 F.2d 438, 164 USPQ 619 (CCPA 1970); and *In re Thorington,* 418 F.2d 528, 163 USPQ 644 (CCPA 1969).

A timely filed terminal disclaimer in compliance with 37 CFR 1.321(c) may be used to overcome an actual or provisional rejection based on a nonstatutory double patenting ground provided the conflicting application or patent is shown to be commonly owned with this application. See 37 CFR 1.130(b).

Effective January 1, 1994, a registered attorney or agent of record may sign a terminal disclaimer. A terminal disclaimer signed by the assignee must fully comply with 37 CFR 3.73(b).

7. Claim 1-46 of the instant application are provisionally rejected under the judicially created doctrine of obviousness type double patenting as being unpatentable over claims 1-2, 4-14, 15-24 and 26-39 of the copending US Application No. 10/458,628.

In particular, Claims 1, 4-7, 10, 13, 20, 23, 26-29, 32 of the instant application are obvious over claims 1-2, 4-5, 12-13, 23-24, 26-27 and 34-39 of the co-pending application No. 10/458,628; Claims 2-3, 8-9, 11-12, 14-19, 24-25, 30-31 and 44-46 of the instant application are obvious over claims 1-2, 4-8, 12-13, 15-16, 19, 23-24, 26, 29-30 and 34-39 of the co-pending application No. 10/458,628; Claims 11-12, 21-22, 33-34, 35-37 of the instant application are obvious over claims 1, 9-12, 20-22 and 31-39 of the co-pending application No. 10/458,628; and Claims 38-43 of the instant application are obvious over claims 34-39 of the co-pending application No. 10/458,628.

Although the conflicting claims are not identical, they are not patentably distinct from each other because all the elements/ features of claim-set of the instant application either exist in similar or different names, closely related in claimed subject matter, and/ or would have been obvious over the conflicting claim-set of the copending application No. 10/458,628.

Differences between the claims 1, 4-7, 10, 13, 20, 23, 26-29 and 32 of the instant application and the conflicting claims 1-2, 4-5, 12-13, 23-24, 26-27 and 34-39 of the co-pending application are that the co-pending application claim set fails to disclose the limitations such as assigning/ configuring a user policy associated with the plurality of the input ports, or user information, and restricting the traffic accordance with the user policy, and if the network access device has enough system resources to dynamically configure the user policy.

However, reference Mao et al teaches assigning/ configuring a user policy associated with the plurality of the input ports, or user information, and restricting the traffic accordance with the

user policy (Col 6, line 63- Col 7, line 40; port or address/ VLAN or zone based policies, and processing packets according to the security policies), and if the network access device has enough system resources to dynamically configure the user policy (Col 4, lines 1-32; Col 5, starts at line 35; determining whether the policy is associated with the particular virtual private network.) Furthermore, conflicting claim set of the co-pending application teaches restricting the traffic if the network access device has enough system resources to dynamically configure the user policy (claims 34-39 of the co-pending application; determining whether switch has enough resources to support VLAN) .

Mao et al and the co-pending application are from the same field of endeavor of network security and managing secure packet processing. Therefore, at the time of invention, it would have been obvious to the ordinary skill in the art to design a device to dynamically assign a user policy to the one of the plurality of input ports and restrict further traffic on the one of the plurality of input ports in accordance with the user policy in order to provide a robust user policy based communication control mechanism.

This is an obvious type double patenting rejection.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

8. Claims 1- 34 and 44-46 are rejected under 35 U.S.C. 103(a) as obvious over Tsuchiya et al (US 7360086 B1) in view of Mao et al (US 7,302,700 B2) further in view of Kameda (US 2003/0028808 A1)

Regarding claim 1, Tsuchiya et al teaches network access device for providing network security, comprising:

a plurality of input ports (Fig 1.21-25; Col 1, starts at line 25; LAN switch with plural ports);

a memory for storing routing data received on the plurality of input ports (Fig 1.11; Col 2, starts at line 32; network device, switch for storing control/ host table, and port information) ;

a switching fabric (Fig 1.11; switch) for routing the data to at least one output port (Fig 7.210; LAN switch with the routing, and port information) and

control logic (Col 2, starts at line 35; Col 7, starts at line 5; authentication, or control information/ table) adapted to:

authenticate a physical address of a user device coupled to one of the plurality of input ports (Col 8, starts at line 5; MAC address authentication);

authenticate user information provided by a user of the user device only if the physical address is valid (Fig 4, steps 102 and 103; Col 8, starts at line 5; Col 14, lines 10-59; authenticating user/source using the authentication table after matching/ checking the MAC address in the host table);

restrict access to the one of the plurality of input ports in accordance with the user information only if the user information is valid (Fig 3; Fig 7; Col 2, lines 32-55;Col 14, lines 40-60; restricting port access based on control, or authentication table)

Tsuchiya et al fails to teach expressly control logic adapted to dynamically assign a user policy to the one of the plurality of input ports and restrict further traffic on the one of the plurality of input ports in accordance with the user policy, and if the network access device has enough system resources to dynamically configure the user policy.

However, Mao et al teaches control logic adapted to dynamically assign a user policy to the one of the plurality of input ports and restrict further traffic on the one of the plurality of input ports in accordance with the user policy (Col 6, line 63- Col 7, line 40; port or address/ VLAN or zone based policies, and processing packets according to the security policies), and if the network access device has enough system resources to dynamically configure the user policy (Col 4, lines 1-32; Col 5, starts at line 35; determining whether the policy is associated with the particular virtual private network.)

Furthermore, in the case, position for the inherency (regarding the above teachings of Tsuchiya et al) is not found supportable Kameda alternatively teaches control logic to authenticate user information provided by a user of the user device only if the physical address is valid (Fig 3, steps S32 and S33; Par 037, 038, 053, 54; authenticating the user once MAC address is authenticated) , and to restrict access to the one of the plurality of input ports in accordance with the user information only if the user information is valid (Fig 1.2 and 51; Par 53-54, 60-62; assigning/ filtering ports according to the user authentication database.)

Mao et al , Kameda and Tsuchiya et al are analogous art because they are from the same field of endeavor of secure network communication. Therefore, at the time of invention, it would have been obvious to a person of ordinary skill in the art to modify Tsuchiya et al 's authentication mechanism with the teachings of Mao et al and/ or Kameda to design a device to dynamically assign a user policy to the one of the plurality of input ports and restrict further

traffic on the one of the plurality of input ports in accordance with the user policy, and wherein authenticate user information provided by a user of the user device only if the physical address is valid with a reasonable degree of success in order to provide a robust communication control mechanism through user policy.

Regarding claim 13, it is rejected applying as above applied rejecting claim 1, furthermore, Tsuchiya et al teaches a method for providing network security, comprising:

authenticating in a network access device a physical address of a user device coupled to a port of the network access device (Col 8, starts at line 5; MAC address authentication);

authenticating user information provided by a user of the user device to the network access device only if the physical address is valid (Fig 4, steps 102 and 103; Col 8, starts at line 5; Col 14, lines 10-59; authenticating user/source using the authentication table after matching/ checking the MAC address in the host table); and

restricting further traffic on the port in accordance with the user information only if the user information is valid (Fig 3; Fig 7; Col 2, lines 32-55;Col 14, lines 40-60; restricting port access based on control, or authentication table.)

Tsuchiya et al fails to teach expressly dynamically assigning a user policy to the port and restricting further traffic on the one of the plurality of input ports in accordance with the user policy, and if the network access device has enough system resources to dynamically configure the user policy.

However, Mao et al teaches dynamically assign a user policy to the one of the plurality of input ports and restrict further traffic on the one of the plurality of input ports in accordance with

the user policy (Col 6, line 63- Col 7, line 40; port or address/ VLAN or zone based policies, and processing packets according to the security policies) and if the network access device has enough system resources to dynamically configure the user policy (Col 4, lines 1-32; Col 5, starts at line 35; determining whether the policy is associated with the particular virtual private network.)

Furthermore, in the case, position for the inherency (regarding the above teachings of Tsuchiya et al) is not found supportable Kameda alternatively teaches control logic to authenticate user information provided by a user of the user device only if the physical address is valid (Fig 3, steps S32 and S33; Par 037, 038, 053, 54; authenticating the user once MAC address is authenticated) , and to restrict access to the one of the plurality of input ports in accordance with the user information only if the user information is valid (Fig 1.2 and 51; Par 53-54, 60-62; assigning/ filtering ports according to the user authentication database.)

Regarding claim 23, it is rejected applying as above applied rejecting claim 1, furthermore, Tsuchiya et al teaches a network system, comprising:

a data communications network (Fig 1; VLAN);

network access device coupled to the data communications network (Fig 1; LAN Switch); and

a user device coupled to a port of the network access device (Fig 1; PC);

wherein the network access device is adapted to authenticate a physical address of the user device (Col 8, starts at line 5; MAC address authentication), to authenticate user information provided by a user of the user device only if the physical address is valid (Fig 4, steps 102 and 103; Col 8, starts at line 5; Col 14, lines 10-59; authenticating user/source using the authentication table after matching/ checking the MAC address in the host table), and to restrict access to the port in

accordance with a user policy associated with the user information only if the user information is valid (Fig 3; Fig 7; Col 2, lines 32-55;Col 14, lines 40-60; restricting port access based on control, or authentication table).

Tsuchiya et al fails to teach expressly access device to dynamically assign a user policy to the port and restricting further traffic on the one of the plurality of input ports in accordance with the user policy, and if the network access device has enough system resources to dynamically configure the user policy.

However, Mao et al teaches network access device adapted to dynamically assign a user policy to the one of the plurality of input ports and restrict further traffic on the one of the plurality of input ports in accordance with the user policy (Col 6, line 63- Col 7, line 40; port or address/ VLAN or zone based policies, and processing packets according to the security policies) and if the network access device has enough system resources to dynamically configure the user policy (Col 4, lines 1-32; Col 5, starts at line 35; determining whether the policy is associated with the particular virtual private network.)

Furthermore, in the case, position for the inherency (regarding the above teachings of Tsuchiya et al) is not found supportable Kameda alternatively teaches control logic to authenticate user information provided by a user of the user device only if the physical address is valid (Fig 3, steps S32 and S33; Par 037, 038, 053, 54; authenticating the user once MAC address is authenticated) , and to restrict access to the one of the plurality of input ports in accordance with the user information only if the user information is valid (Fig 1.2 and 51; Par 53-54, 60-62; assigning/ filtering ports according to the user authentication database.)

Regarding claim 2, Tsuchiya et al teaches the network access device wherein the physical address comprises a Media Access Control (MAC) address (Col 1, starts at line 25; MAC address).

Regarding claim 3, Tsuchiya et al teaches the network access device wherein the control logic is adapted to authenticate the user information (Fig 3; Col 2, starts at line 32). Tsuchiya et al fails to teach utilizing IEEE 802. lx protocol. However, examiner takes an official notice on that at the time of invention, use of IEEE 802. lx protocol in wireless/ VLAN security was well known in the art (see US 7188364 B2). Therefore, it would have been obvious to an ordinary skill in the art to design the authentication mechanism accordance with the IEEE 802. lx protocol in order to provide an alternative and robust authentication mechanism.

Regarding claim 4, Tsuchiya et al teaches the network access device wherein the user policy identifies an access control list (Fig 3; Col 2, starts at line 35; authentication unit utilizing control, or authentication table, or host table).

Regarding claim 5, Tsuchiya et al teaches the network access device wherein the user policy includes an access control list (Fig 3; Col 2, starts at line 35; control, or authentication table).

Regarding claim 6, Tsuchiya et al teaches the network access device wherein the user policy identifies a Media Access Control (MAC) address filter (Fig 2; MAC address in host table).

Furthermore, Kameda teaches the network access device wherein the user policy identifies a Media Access Control (MAC) address filter (Fig 1.22; MAC address filter in switch table)

Regarding claim 7, Kameda teaches the network access device wherein the user policy includes a Media Access Control (MAC) address filter (Fig 1.22; MAC address filter in switch table).

Regarding claim 8, Kameda teaches the device wherein the control logic is adapted to send user information to an authentication server and to receive an accept message from authentication server if the user information is valid (Fig 1; authentication server; Fig 1.2 and 51; Par 53-54, 60-62; assigning/ filtering ports, MAC addresses according to the authentication database).

Regarding claim 9, Kameda teaches the network access device of claim 8, wherein the authentication server comprises a Remote Authentication Dial-In User Service (RADIUS) server (Fig 1; Par 012,037; remote authentication server).

Regarding claim 10, it is rejected applying as above applied rejecting claim 9, furthermore, Kameda teaches the network access device wherein the accept message includes the user policy (Fig 1; authentication server table including authentication response information; Fig 1.2 , 5 and 51; Par 53-54, 60-62; server authentication database)

Regarding claim 11, Tsuchiya et al teaches the network access device wherein the control logic is further adapted to assign the one of the plurality of input ports to a virtual local area network (VLAN) associated with the user information if the user information is valid (Fig 2; Col 1, starts at line 16; authenticating VLAN information).

Regarding claim 12, Tsuchiya et al teaches the network access device wherein the control logic is adapted to receive a message from an authentication server, wherein the message comprises a VLAN identifier (ID) associated with the user information, and to assign the one of the plurality of input ports to a VLAN associated with the VLAN ID (Fig 2; Col 1, starts at line 16; authenticating VLAN information/ number).

Regarding claim 44, Tsuchiya et al teaches the device wherein the user information comprises a user name and a password (Fig 3; Col 8, lines 40-50)

Regarding claims 14-22, 24-34 and 45-46, they recite the limitations of claims 1-13, 23 and 44, therefore, they are rejected applying as above applied rejecting claims 1-13, 23 and 44.

Allowable Subject Matter

9. Claims 35-37 would be allowable if rewritten, or filed a signed terminal disclaimer to overcome the obviousness type Double Patenting rejections, set forth in this Office action and to include all of the limitations of the base claim and any intervening claims.

10. Claims 38-43 would be allowable if rewritten or amended, or filed a signed terminal disclaimer to overcome the obviousness type Double Patenting rejections, set forth in this Office action.

Conclusion

11. Examiner's note: Examiner has cited particular columns and line numbers in the references as applied to the claims above for the convenience of the applicant. Although the specified citations are representative of the teachings in the art and are applied to the specific limitations within the individual claim, other passages and figures may be applied as well. It is respectfully requested from the applicant, in preparing the responses, to fully consider the references in entirety as potentially teaching all or part of the claimed invention as well as the context of the passage as taught by the prior art or disclosed by the Examiner.

12. A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Shanto M Z Abedin whose telephone number is 571-272-3551. The examiner can normally be reached on M-F from 10:30 AM to 7:30 PM. If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Moazzami Nasser, can be reached on 571-272-4195. The fax phone number for the organization where this application or

proceeding is assigned is 703-872-9306. The RightFax number for faxing directly to the examiner is 571-273-3551.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Shanto M Z Abedin

Examiner, AU 2436

/Nasser G Moazzami/

Supervisory Patent Examiner, Art Unit 2436